

FILED

## UNITED STATES DISTRICT COURT

## EASTERN DISTRICT OF VIRGINIA

Alexandria Division

2011 FEB -7 P 4:46

CLERK US DISTRICT COURT  
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE	)	
§2703(d) ORDER RELATING TO	)	MISC. NO. 10GJ3793
TWITTER ACCOUNTS:	)	No. 1:11DM3 (Judge Buchanan)
WIKILEAKS, ROP_G; IOERROR;	)	
AND BIRGITTAJ	)	Hearing: February 15, 2011
	)	10:30 a.m.
	)	
	)	<b>UNDER SEAL</b>

**GOVERNMENT'S OBJECTION TO MOTION OF THREE TWITTER  
SUBSCRIBERS TO VACATE ORDER OF DECEMBER 14, 2010, UNDER § 2703(d)**

The United States of America, by and through Neil H. MacBride, United States Attorney, Eastern District of Virginia, and John S. Davis, Assistant United States Attorney, objects as follows to the Motion of Real Parties in Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14, 2010 Order:

**I. *Background***

On December 14, 2010, this Court entered a sealed order (the Order) pursuant to 18 U.S.C. § 2703(d) directing Twitter, Inc., to disclose certain non-content records and other information pertaining to Twitter accounts, including those identified as rop\_g; ioerror; and birgittaj. For each account, the Order specified the following customer or subscriber information, for the period November 1, 2009, to the date of the Order:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

21

6. means and source of payment for such service (including any credit card or bank account number) and billing records.

The Order also identified additional records, for the same Twitter accounts and same time period:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

On January 5, 2011, this Court unsealed the Order (but no other document in this matter), and authorized Twitter to disclose it. Twitter thereafter gave notice of the Order to the affected account holders, including the three “real parties in interest,” who are movants here: Jacob Appelbaum (associated with ioerror), Birgitta Jonsdottir (associated with birgittaj), and Rop Gonggrijp (associated with rop\_g) (collectively, the Subscribers).

After discussions with counsel, on January 12, 2011, the government agreed with Twitter to a narrowing of the terms of the Order, reducing the number of records to be disclosed.<sup>1</sup> On

---

<sup>1</sup>On or about January 12, 2011, the government informed Twitter and the Subscribers that it agreed to the following with respect to the Order: 1. The government expected Twitter to provide information covered by the Order only for the four listed Twitter accounts (Wikileaks, rop\_g, ioerror, and birgiittaj) between November 15, 2009 and June 1, 2010; 2. to the extent Twitter has no information responsive to certain parts of the Order, for example credit card information, it need not provide such information; 3. the government had not sought and did not expect to receive the contents of any communications; 4. the government did not expect Twitter to provide records that would be unusually voluminous in nature or would otherwise cause an undue burden to produce. Twitter should let the government know if it believed any portion of the Order would be unduly burdensome after consultation with its engineers. For example, the government did not expect Twitter to produce the records of user activity for any connections to or from the Account relating to public followers of a Twitter account, Apache logs, or replies to Twitter feeds; 5. the government and Twitter understood that the records of user activity for any connections to or from the Account would include the IP addresses of the Account holder’s

January 26, 2011, the Subscribers moved to vacate the Order, citing a variety of statutory and constitutional grounds. The government hereby objects to the Subscribers' motion.

## II. *Argument*

### A. **Section 2703(d) Does Not Authorize the Subscribers to Challenge a "Non-Content" Order For an Alleged Non-Constitutional Violation of the Statute, and, in Any Event, This Court Has Already Determined That the Order is Based Upon "Specific and Articulate Facts."**

The Subscribers first argue that no "specific and articulable facts" demonstrate that the Twitter records identified in the Order are "relevant and material" to a criminal investigation, as § 2703(d) requires. Although they are not privy to the Order's factual basis (which remains sealed), the Subscribers contend that because their "Tweets" covered a "broad range of non-WikiLeaks topics," the records identified in the Order necessarily include data "that has no connection whatsoever to WikiLeaks and cannot be relevant or material to any investigation." (Mot. Vacate at 6-7.) Accordingly, say the Subscribers, the Order must be vacated and the government's application disclosed, to allow them "a fair opportunity to challenge the Government's assertions and highlight any material misstatements or omissions." (Mot. Vacate at 7.)

---

logins; and 6. the government believed that the records of user activity for any connections to or from the Account would include non-content information relating to direct messages between the four accounts listed in the Order (Wikileaks, rop\_g, ioerror, and birgiittaj), for example non-content information reflecting the fact that a message was passed between such accounts. The government also understood that Twitter was looking into whether it agreed that the Order covered such connection records and whether it was possible to produce them from an engineering standpoint. The government confirmed that it was not seeking any information (content or non-content) relating to direct messages except those exchanged among any of the four accounts listed in the Order.

The Subscriber's statutory claim is meritless. As this Court has already determined, the government's application for the Order (the Application) satisfied the governing standard by alleging "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." (Order at 1.) The Order is therefore fully compliant with § 2703(d), and the Court should reject the Subscribers' speculation that the Application "likely contains material errors or omissions" that render it insufficient. (Mot. Vacate at 1.)

Several additional reasons require rejection of the Subscribers' § 2703(d) argument. In the first place, the Subscribers cannot move to vacate the Order on statutory grounds. The Order was issued under 18 U.S.C. § 2703(d), which is part of the Stored Communications Act (18 U.S.C. §§ 2701-12) (the SCA). That Act expressly prohibits the improvising of remedies. Specifically, Congress provided that "[t]he remedies and sanctions described in [the SCA] are the only judicial remedies and sanctions for nonconstitutional violations of [the SCA]." 18 U.S.C. § 2708; *see United States v. Clenney*, No. 09-5114, slip op. at 13 (4<sup>th</sup> Cir. Feb. 3, 2011). Thus, because the Subscribers' first argument alleges a nonconstitutional violation of § 2703(d), they may invoke only the "judicial remedies" described in the SCA to address the putative illegality. Accordingly, in challenging the Order based on an alleged violation of the § 2703(d) standard, the Subscribers must identify authority in the SCA that permits such a motion in the first place. But the Subscribers have failed to do so, and with good reason – the SCA does not authorize them to move to vacate the Order for a nonconstitutional § 2703(d) violation.

The SCA provides only two ways to challenge a § 2703(d) order. First, the "service provider" may move to quash or modify the order "if the information or records requested are

unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.” 18 U.S.C. § 2703(d). This remedy would theoretically be available to Twitter, the named service provider, but it is not available to the Subscribers.

Second, a “subscriber or customer” may move to vacate an order, but only under certain conditions, including when the order seeks the contents of that subscriber or customer’s communications. *See* 18 U.S.C. § 2704(b)(1)(A) (motion to vacate must state “that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought”). Here, of course, the Order seeks only “non-content” records and information about the Subscribers’ Twitter accounts.

Notably, subscribers are not entitled to notice that the government has sought disclosure of non-content information under § 2703(c), as the government has here. *See* 18 U.S.C. § 2703(c)(3) (“A governmental entity receiving records or information under this section is not required to provide notice to a subscriber or customer”). On the other hand, if the government were seeking content information under Section 2703(b), notice (albeit notice that may be delayed) is required unless a search warrant is obtained. *See* 18 U.S.C. § 2703(b)(1). Since Congress required that subscribers be notified only when content is disclosed, it makes sense that Congress provided subscribers with the ability to contest only such disclosures. *See Clenney*, No. 09-5114, slip op. at 12 (noting that statute “draws a distinction between the content of a communication and the records pertaining to a communication service account”).<sup>2</sup>

---

<sup>2</sup>If the Subscribers have been aggrieved by a wilful violation of the SCA, they may sue the United States for money damages under 18 U.S.C. § 2712. Challenging the Order in the manner chosen here, however, is simply not among the options Congress authorized.

The above-described legal framework comports with practical demands and with common sense. Pre-indictment challenges can interfere with ongoing criminal investigations, and Congress carefully and appropriately tailored the ability to challenge the government's acquisition of non-content information. Because the Subscribers cannot avail themselves of the only remedies set forth in the SCA, the Subscribers have no basis to move to vacate the Order on statutory grounds.

Moreover, even assuming that the procedures in § 2704(b) were available to the Subscribers, any challenge to the Order under § 2704(b) would fail. That section provides that a motion to vacate must be denied if “there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry.” 18 U.S.C. § 2704(b)(4). In this case, any motion to vacate the Order under § 2704(b) would be denied because in the Order this Court has already concluded that the government satisfied the higher § 2703(d) standard of providing “specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.”<sup>3</sup>

---

<sup>3</sup>By its terms, section 2704(b) does not permit customers to contest whether the records sought by a § 2703(d) order are *material* to an investigation, and legislative history confirms that Congress intended not to provide customers with this authority. As described above, until 1994, the standard for issuing a § 2703(d) order was identical to that for evaluating a § 2704(b) challenge: in both cases, courts had to determine whether the records sought were “relevant to a legitimate law enforcement inquiry.” See Pub. L. 99-508, Title II, § 201, Oct. 21, 1986, 100 Stat. 1861. In 1994, Congress changed the § 2703(d) standard to require that the records be “relevant and material to an ongoing criminal investigation,” but left § 2704 unchanged, thereby precluding customers from employing the new materiality standard in § 2704 litigation. See Pub.L. 103-414, Title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292.

Lacking a legitimate statutory remedy, the Subscribers instead ask the Court to review its own issuance of the Order *de novo* and evaluate, again, whether the Application meets the “specific and articulable facts” standard in 18 U.S.C. § 2703(d). (Mot. Vacate at 4-6.) For all the reasons set forth above, the SCA does not allow the Subscribers to seek such a review. Further, even if this Court were to reconsider the Application, it would find it more than sufficient to meet the § 2703(d) standard. Specifically, as narrowed by the government’s agreement with Twitter, the Order seeks certain non-content business records that may be obtained via a subpoena with no threshold showing to the court, namely (a) subscriber information, including the subscriber’s name, address, connection records, subscriber number, and length of service; and (b) correspondence and records relating to an account. These types of business records can be routinely obtained from providers by subpoena, and the Subscribers have no reasonable expectation of privacy in them. *See Clenney*, No. 09-5114, at 11 (recognizing that under § 2703(c)(2) government can bypass warrant or court order procedures “and simply subpoena the records if it seeks only basic subscriber information, such as the name and address of the customer and telephone call logs”); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (individual had no subjective or reasonable expectation of privacy in his internet and phone “subscriber information,” i.e. his name, email address, telephone number and physical address, when he voluntarily conveyed this information to internet and telephone companies) (citing *Smith*, 442 U.S. at 744, and *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008)).

Further, the following non-content information is the only material sought from Twitter that required the government to show specific and articulable facts to support a reason to believe

that such information was relevant and material to an ongoing criminal investigation. (The Application adequately established this, as this Court has already found.) As narrowed by the government's agreement, see note 1 *supra*, the Order requires disclosure of the following non-content information:

1. Records of user activity for connections made between the four listed accounts (to or from), including IP addresses (which are akin to telephone numbers for a computer), and dates and times (this would include the IP addresses of direct (private) twitter messages between the relevant accounts, for example); and
2. non-content information associated with the contents of communications or stored files (this would include, for example, the IP address of the recipient of a direct message to the extent that recipient is also an account user).

At least one court has ruled that “the ‘specific and articulable facts’ standard derives from the Supreme Court's decision in *Terry*.” *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (citing *Terry v. Ohio*, 392 U.S. 1 (1968)). It follows that “this standard is a lesser one than probable cause.” *In re Application of United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*, 620 F.3d 304, 313 (3d Cir. 2010) (*Third Circuit Opinion*); see *United States v. Warshak*, — F.3d —, 2010 WL 5071766, at \*16 (6<sup>th</sup> Cir. Dec. 14, 2010) (noting “diminished standard that applies to § 2703(d) applications”); see also S. Rep. No. 99-541, at 44-45 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3598-99. The *Terry* standard is met “when an officer ‘point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity.’” *United States v. Mason*, 628 F.3d 123, 128 (4th Cir. 2010) (quoting *United States v. Branch*, 537 F.3d 328, 336 (4th Cir. 2008)).

The Subscribers imply that the “specific and articulable facts” standard is more onerous

than the *Terry* rule (Mot. Vacate at 5), but they identify no court that has adopted this position, and the government is aware of none. The presence of the word “material” in 18 U.S.C. § 2703(d) does not transform the § 2703(d) standard into one that requires a showing that the records sought are “vital,” “highly relevant,” or “essential,” as the Subscribers suggest. (Mot. Vacate at 5.) The Subscribers’ contrary argument is based on cases that discuss “materiality” in contexts very different from § 2703(d). *See* (Mot. Vacate at 5); *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867-73 (1982) (evaluating whether deportation of potential witnesses violated defendant’s constitutional rights); *Roviaro v. United States*, 353 U.S. 53, 62-65 (1957) (evaluating whether government could withhold identity of undercover informer); *United States v. Smith*, 780 F.2d 1102, 1109 (4th Cir. 1985) (evaluating whether government could preclude defendant from introducing classified information at trial). Here, the facts described in the Application fully meet the *Terry* standard and therefore satisfy § 2703(d)’s requirements. *Mason*, 628 F.3d at 128.

Further, there is no merit to the Subscribers’ claim that the records described in the Order cannot be “relevant and material to an ongoing criminal investigation” simply because some of them relate to communications “that have nothing whatsoever to do with WikiLeaks.” (Mot. Vacate at 6.) By the Subscribers’ logic, the government could never use a § 2703(d) order to obtain email transaction logs or phone bills unless the government could show that every email or phone call related directly to the crime under investigation. And their position has radical practical implications. Should providers be required in the first instance to review individual transaction records to determine relevancy? Providers are singularly ill-equipped to determine precisely what information would be relevant to an ongoing investigation. The government is

aware of no court that has adopted such a restrictive and impractical view of § 2703(d). Nor is such a view required by law. See *In re Subpoena Duces Tecum*, 228 F.3d at 348-49 (in explaining that subpoenas are less intrusive than search warrants and therefore require a lower standard, noting that “[t]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists”) (quoting *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991)). Contrary to the Subscribers’ assertions, the Order requires the production of very limited transactional information that is directly relevant and material to the ongoing criminal investigation. This is especially true since with the government’s agreement the Order is limited to connection information between the identified account holders.

In summary, because the SCA strictly limits the remedies available to subscribers whose non-content information is sought, the Subscribers cannot challenge this Court’s finding under § 2703(d) that “specific and articulable facts” support the Order. And even if they could mount such a challenge, it would fail, since the facts in the Affidavit are more than sufficient.

**B. The Order Does Not Infringe Upon Any First Amendment Rights Held by the Subscribers.**

The Subscribers next protest that the Order, which seeks limited subscriber information, such as names and addresses, and transactional records, such as connection data, all of which are business records of Twitter but not the content of the Subscribers’ communications, “threatens the Parties’ protected First Amendment rights.” (Mot. Vacate at 7.)<sup>4</sup> The Subscribers accuse the

---

<sup>4</sup>Neither Mr. Gonggrijp nor Ms. Jonsdottir appears to be a United States citizen. Additionally, no information, whether in their filing or within the government’s knowledge, suggests that either of them maintained a significant continuing presence in the United States during the period of the

government of undertaking a “fishing expedition” that may chill their rights “to speak freely and associate with others.” (Mot. Vacate at 8.) They conclude that under the First Amendment, unless the government can show that the information sought “would further a compelling interest,” and that its request is “the least restrictive way to serve that interest,” the Order must be vacated. (Mot. Vacate at 10.)

But the Subscribers’ argument is long on rhetoric and short on facts demonstrating an actual “chill” on First Amendment freedoms. In reality the Order, which is not conceptually different from a routine subpoena seeking telephone subscriber information and toll records from a telephone company, in no way inhibits the exercise of First Amendment rights.

Moreover, the Parties cannot demonstrate that they are entitled to “particular scrutiny” of the Order based on alleged First Amendment interests. (Mot. Vacate at 8.) The Fourth Circuit has specifically declined to apply the “substantial relationship” test, which balances First Amendment freedoms against the government’s interest in investigating crime, to a grand jury subpoena seeking corporate records of a distributor of sexually explicit films. *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d 229, 234 (4<sup>th</sup> Cir. 1992). Instead, the court directed the district court to “balance the possible constitutional infringement and the government’s need for

---

investigation. There is a legitimate question whether the rights under the Constitution of non-citizen, non-national, non-residents of the United States are substantially identical to those of citizens, residents, or individuals acting within the United States. *See, e.g., United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990) (textual analysis of Constitution “suggests that ‘the people’ protected by the Fourth Amendment, and by the First and Second Amendments . . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community”). Mr. Gonggrijp and Ms. Jonsdottir do not address this threshold question before making arguments that imply that the First and Fourth Amendments apply to them just as they do to Mr. Appelbaum (who is a United States citizen). In any event, for the reasons set forth *infra*, none of the Subscribers identifies a constitutional violation warranting the extraordinary relief that they seek.

documents” when ruling on the motion to quash, “on a case-by-case basis and without putting any special burden on the government.” *Id.*

Doubtless, as the Subscribers assert, the freedoms of speech and association constitute important rights protected by the First Amendment. But, setting aside legal platitudes, the Subscribers fail to present a cognizable First Amendment claim. The irony presented in this case is that the Subscribers publicly posted their Tweets -- the contents of their messages -- on the Internet. Information about the Subscribers’ Twitter followers was also public, since the followers of the Subscribers’ Tweets posted their replies on the Internet. Thus, although the Subscribers claim otherwise, the government has not embarked on a “fishing expedition into information about their postings.” (Mot. Vacate at 8.) Nothing remains to fish for, since the Subscribers and their associates have already made their postings available for all the world to see, and can have no expectation of privacy in them. Nor does the government seek the contents of any of the Subscribers’ private direct messages (akin to private Internet chats), or seek to identity others with whom the Subscribers communicated by direct messages. (Mot. Vacate at 8.) As narrowed by the government’s agreement with Twitter, the Order’s scope extends only to non-content connection records for past communications involving the identified account holders. It does not seek prospective connection records, or attempt to identify the Subscribers’ associates. It does not control or direct the content of the Subscribers’ speech, or restrain, punish or burden any speech or association in which the Subscribers may have engaged. For good reason, the Subscribers fail to explain how the Order chills their freedom of speech or association: they cannot. *See Univ. of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 197-98 (1990) (subpoena for academic papers did not impose content-based or direct burden on university);

*Branzburg v. Hayes*, 408 U.S. 665, 682, 691 (1972) (requiring reporter to comply with subpoena “involves no restraint on what newspapers may publish, or on the type or quality of information reporters may seek to acquire,” nor does it threaten “a large number or percentage of all confidential news sources”).

Thus, even if the “substantial relationship” test were required in the Fourth Circuit -- which it is not -- since enforcement of the Order will not chill speech or association, that test would not apply. *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d at 234 (following *Branzburg* and *University of Pennsylvania*). To the extent that the provider, Twitter, stands in the same shoes as an ordinary citizen before this Court, “neither the First Amendment nor any other constitutional provision protects [it] from disclosing to a grand jury information that [it] has received in confidence,”<sup>5</sup> absent a showing of harassment or bad faith. *Branzburg*, 408 U.S. at 682, 707; *Univ. of Pennsylvania*, 493 U.S. at 201 n.8 (1990) (implying that “the bad-faith exercise of grand jury powers” is the only basis for a First Amendment challenge to a subpoena); *In re Shain*, 978 F.2d 850, 852 (4th Cir. 1992).

Finally, the Subscribers do not allege -- and cannot show -- that the government has acted in bad faith, either in conducting its criminal investigation or in obtaining the Order. The government described the nature of its investigation in its Application, allowing the Court to assess the legitimacy of the case before deciding to issue the Order. The government’s decision

---

<sup>5</sup>Most cases that evaluate First Amendment challenges to the compelled disclosure of documents involve subpoenas, rather than court orders. Court orders issued under 18 U.S.C. § 2703(d), such as the Order, are similar to subpoenas because they also require the disclosure of documents, but they are arguably more protective of citizens’ interests because they are subject to prior judicial review and require a higher factual showing for issuance. Accordingly, a party attempting to challenge a § 2703(d) court order should be subject to standards that are at least as stringent as those applied to a motion to quash a subpoena.

to pursue the particular records described in the Order was also subject to oversight by this Court, which concluded that the Order was warranted because the government “offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). The government has acted in good faith throughout, and there is no evidence that either the investigation or the Order is intended to harass the Subscribers or anyone else. *See In re Grand Jury* 87-3, 955 F.2d at 233 n.3 (noting that there was no allegation of grand jury bad faith); *United States v. Steelhammer*, 539 F.2d 373, 376 (4th Cir. 1976) (Winter, J., dissenting), *adopted by the court en banc*, 561 F.2d 539, 540 (4th Cir. 1977) (“[T]he record fails to turn up even a scintilla of evidence that the reporters were subpoenaed to harass them or to embarrass their newsgathering abilities . . .”). Accordingly, the Subscribers have no colorable First Amendment claim justifying vacation of the Order.

**C. Because the Subscribers Have No Expectation of Privacy in Their IP Addresses Provided to Twitter, the Order Does Not Violate Their Fourth Amendment Rights.**

The Court should likewise reject the Subscribers’ claim that the Order threatens their Fourth Amendment rights. The Subscribers identify only one aspect of the Order that supposedly implicates such rights: its directive that Twitter produce the Internet Protocol (“IP”) addresses that the Subscribers used to log in to their Twitter accounts at particular dates and times. (Mot. Vacate at 10.) According to the Subscribers, this IP address information, in connection with the dates and times of the account logins, implicates the Fourth Amendment because it “could allow the government to discern the physical location of the parties at the exact time they were

publishing on Twitter.” *Id.* However, even assuming for argument’s sake that the Subscribers have standing to bring a Fourth Amendment challenge to the Order, the Subscribers have no Fourth Amendment interest in IP address information, and the Order cannot not be vacated on that ground.

IP addresses are analogous to telephone numbers. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Just as every telephone is assigned a number that phone companies use to route calls, every computer directly connected to the Internet is assigned an IP address that “serves as the routing address for email, pictures, requests to view a web page, and other data sent across the Internet.” *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409 (2d Cir. 2004). “Like telephone numbers, . . . IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers.” *Forrester*, 512 F.3d at 510. Accordingly, the government’s acquisition of IP address information is properly analyzed using the same legal framework that applies to the government’s acquisition of phone numbers. *See id.* (concluding that real-time collection of IP addresses of websites visited by Internet user was “constitutionally indistinguishable” from the use of a pen register to collect numbers dialed from a phone line).

Because IP addresses are analogous to phone numbers and should be governed by the same legal rules, *Smith v. Maryland*, 442 U.S. 735 (1979), disposes of the Subscribers’ Fourth Amendment claim. In *Smith*, the Supreme Court concluded among other things that telephone users had no reasonable expectation of privacy in the telephone numbers they dialed because they “voluntarily conveyed numerical information to the telephone company” and thereby “assumed the risk that the company would reveal to police the numbers . . . dialed.” 442 U.S. at 744. This

conclusion is consistent with the general rule that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44 (citing cases); *see also United States v. Miller*, 425 U.S. 435, 440 (1976) (bank depositor had no “legitimate expectation of privacy” in financial information “voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business”); *Bynum*, 604 F.3d at 164 (internet user had no legitimate expectation of privacy in subscriber information that he voluntarily conveyed to his internet company). Just as telephone users voluntarily transmit phone numbers to their phone providers, the Subscribers voluntarily transmitted their IP addresses to Twitter to gain access to their Twitter accounts, thereby assuming the risk that Twitter would reveal the addresses to law enforcement agents. *See Forrester*, 512 F.3d at 510. Indeed, Twitter’s Privacy Policy places all users on notice that Twitter servers “automatically record information (‘Log Data’) created by your use of the Services,” and specifies that this Log Data “may include information such as your IP address.” Twitter Privacy Policy, <http://twitter.com/privacy> (last visited February 1, 2011). Accordingly, based on the Supreme Court’s reasoning in *Smith*, the Subscribers cannot now claim a reasonable expectation of privacy in Twitter’s records of their IP addresses.<sup>6</sup>

To the government’s knowledge, no court has concluded that Internet users have a

---

<sup>6</sup>Even if the Subscribers somehow had a reasonable expectation of privacy in their IP address information, the Order would not be improper under the Fourth Amendment. *See Smith*, 442 U.S. at 744 (“[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.”); *S.E.C. v. Jerry T. O’Brien, Inc.*, 467 U.S. 735, 743 (1984) (past Supreme Court rulings “disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers”); *Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946) (explaining Fourth Amendment requirements for subpoenas).

reasonable expectation of privacy in IP address records. Indeed, at least two courts of appeals have affirmatively held that Internet users have no reasonable expectation of privacy in IP address information.<sup>7</sup> See *Forrester*, 512 F.3d at 510 (“[E]-mail and Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.”); *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (“[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs.”). This Court should adopt the reasoning of these cases and hold that the Subscribers lack a reasonable expectation of privacy in their IP address information.

Moreover, there is no merit to the Subscribers’ suggestion that the Court should depart from these cases and conclude that IP address records deserve Fourth Amendment protection because they “could allow the government to discern the physical location of the [Subscribers] at the exact time they were publishing on Twitter.” (Mot. Vacate at 10.) Business records do not become privileged merely because they contain information that might enable the government to

---

<sup>7</sup>The Subscribers do not address these cases and instead imply in a footnote that only opinions “specifically addressing Twitter data” are directly on point. (Mot. Vacate at 12 n.10.) But there is no legal basis for distinguishing Twitter’s IP address records from the IP address records of any other Internet service provider. In any event, cases that analyze the collection of IP address information are much more relevant to the Subscribers’ Fourth Amendment argument than the cases cited by the Subscribers in the same footnote, which evaluate government searches of computers seized from private homes and government efforts to obtain the content of email messages. See *Trulock v. Freeh*, 275 F.3d 391, 402-03 (4th Cir. 2001) (consent-based search of home, computer, and computer files); *United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) (warrant-based search of computers seized from defendant’s home); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (same); *United States v. Warshak*, --- F.3d ---, 2010 WL 5071766, at \*11, \*14 (6th Cir. Dec. 14, 2010) (use of § 2703 process to obtain content of email messages).

discern a person's location. For example, traditional land-line telephone records reveal that a caller was using a particular land-line telephone number at a particular time, and investigators have long been able to use such information to place a caller in a particular location (often a private home) at the time of the call. However, telephone users have no reasonable expectation of privacy in this land-line information, even when collected in real-time, when the government obtains it from the phone provider. *See Smith*, 442 U.S. at 745 (concluding that phone user had no legitimate expectation of privacy in phone numbers he dialed); *Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d 1030, 1046 n.49 (D.C. Cir. 1978) (citing cases for proposition that telephone subscribers have no Fourth Amendment basis for challenging government inspection of their toll records). In this respect, IP address connection records are no different than land-line telephone records, except that they are *less* geo-specific, not more, since many computers are considerably more mobile than land-line telephones. Further, the government is not required to obtain a warrant before compelling businesses to produce other types of business records from which location-based inferences could be drawn, such as bank records, employment records, credit card records, and other records of customer purchases. *See, e.g., Miller*, 425 U.S. at 444 (rejecting Fourth Amendment challenge to subpoena for bank records). In short, the Subscribers do not have a Fourth Amendment interest in Twitter's records of their IP addresses even if the government could use these records to discern the Subscribers' locations at certain times.

The cases cited by the Subscribers do not support their claim that they have a Fourth Amendment interest in Twitter's IP address records. First, *United States v. Karo*, 468 U.S. 705 (1984), requires the government to obtain a warrant before using a tracking device to reveal

information about the interior of a private location. 468 U.S. at 715. But neither the Supreme Court nor the Fourth Circuit has applied this tracking-device standard to business records, even though many kinds of business records could reveal someone's location at a particular time. Indeed, if *Karo* did apply to business records, it would implicitly overrule *Smith v. Maryland*, *United States v. Miller*, and other Supreme Court cases that have upheld the government's ability to obtain business records without a warrant. Plainly, *Karo* did not void all of this settled precedent.

Furthermore, applying the *Karo* standard to all business records would have absurd and unworkable results. For example, the government would have to obtain a warrant, rather than a subpoena, to require a company to disclose phone records, security surveillance videos, visitor sign-in sheets, or even time-stamped photographs of an employee in her office, because any of these records could reveal someone's location in a private space at a particular time. *See United States v. Gray*, 491 F.3d 138, 153 (4th Cir. 2007) (citing *O'Connor v. Ortega*, 480 U.S. 709 (1987)) (“[A]n individual can have an expectation of privacy in his workplace.”). The logical result of such an expansion of *Karo* would be that the government would be required to use a warrant, rather than a subpoena, whenever it sought to obtain business records. The Fourth Amendment has never been so construed.

Even if the *Karo* tracking-device standard were somehow applicable here, the Subscribers still would have no Fourth Amendment interest in Twitter's records of their IP addresses. Although the government must obtain a warrant to use a tracking device to “reveal a critical fact” about the interior of a private home, *Karo*, 468 U.S. at 715, no warrant is required when the government obtains more generalized information about a tracking device's location, even when

the device is actually located in a private space.<sup>8</sup> *See id.* at 720 (finding no Fourth Amendment violation when government used tracking device to determine that can of ether was inside warehouse because, *inter alia*, the device “did not identify the specific locker in which the ether was located”). Twitter’s IP address records, without more, do not reveal the type of precise location information protected by the *Karo* standard. *See* (Mot. Vacate at 11 n.9 (“[O]ne of the leading companies advertises that its free geolocation tool can determine the location of ‘79% [of U.S. IP addresses] within a 25 mile radius.’”).) Accordingly, even if *Karo* applied to business records, the Subscribers have failed to establish that the government’s acquisition of Twitter IP address records would violate a Fourth Amendment right under *Karo*. *Cf. United States v. Ortega-Estrada*, 2008 WL 4716949, at \*13 (N.D. Ga. Oct. 22, 2008) (finding that even GPS information accurate to within 32 meters “revealed only a general area where the suspect was at a particular time, and thus, did not invade a place where he might have an expectation of privacy”).

The *Third Circuit Opinion*, on which the Subscribers principally rely, also does not help their cause. (Mot. Vacate at 13.) In that case, the court agreed that the privacy interests at issue in *Karo* “are confined to the interior of the home,” *Third Circuit Opinion*, 620 F.3d at 312, and it declined to hold that probable cause was always required for the government’s collection of historical cell-site location information (CSLI) because there was no evidence in the record that

---

<sup>8</sup>The Subscribers cite a recent D.C. Circuit decision, *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), which suggests that the continued use of a tracking device in public may raise additional issues under the Fourth Amendment. (Mot. Vacate at 14.) In addition to being inapplicable here, this decision is inconsistent with Supreme Court precedent, including *Smith v. Maryland* and *Katz v. United States*, 389 U.S. 347 (1967), and conflicts with tracking-device decisions of three other courts of appeals. *See United States v. Marquez*, 605 F.3d 604, 609-10 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1216-17 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994, 997-98 (7th Cir. 2007).

historical CSLI revealed information about the interior of a home.<sup>9</sup> *See id.* at 313. Likewise, the Subscribers have presented no evidence that Twitter's IP address records would reveal information about the interiors of their homes. Furthermore, even if the Third Circuit's opinion were persuasive and binding on this Court, *cf.* 620 F.3d at 320 (Tashima, J., concurring) (noting that majority opinion "vests magistrate judges with arbitrary and uncabined discretion to grant or deny issuance of § 2703(d) orders at the whim of the magistrate, even when the conditions of the statute are met" (footnote omitted)), its reasoning is inapplicable to the collection of IP addresses because such addresses are much more analogous to the phone numbers collected in *Smith v. Maryland* than they are to CSLI. Accordingly, even though the Third Circuit concluded that *Smith* is inapplicable to CSLI (a conclusion with which the government disagrees), it does not follow that *Smith* is inapplicable to IP address records.<sup>10</sup> In fact, just eight days after issuing the *Third Circuit Opinion*, the Third Circuit cited *Smith* in support of its conclusion that "no reasonable expectation of privacy exists in an IP address." *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010).

In summary, for all of these reasons, the Order does not implicate the Subscribers' Fourth Amendment rights, and cannot be vacated on that ground.

#### **D. Having Properly Issued the Order, This Court Need Not**

<sup>9</sup>Records of CSLI reveal among other things the location of the antenna tower that carried a given call at a particular date and time. *See Third Circuit Opinion*, 620 F.3d at 308.

<sup>10</sup>The Third Circuit distinguished *Smith* on the ground that cell-phone customers do not "voluntarily" share CSLI with their phone providers. *See Third Circuit Opinion*, 620 F.3d at 317-18. This basis for distinguishing *Smith* is not available to the Subscribers because, as discussed above, they voluntarily conveyed their IP address information to Twitter when they logged into their Twitter accounts. Moreover, in an increasingly tech-savvy world, the notion, baldly asserted by the Subscribers, that a typical Internet user has no awareness that his IP address is transmitted to the Internet sites with which he or she communicates (such as Twitter), is dubious at best. (Mot. Vacate at 14.)

**Reconsider Its Decision and Should Reject the Subscribers’  
Constitutional Avoidance Argument.**

The Subscribers next ask the Court to apply the doctrine of constitutional avoidance in light of a § 2703(d) application that supposedly “raises serious constitutional questions,” and to vacate the Order and require that the government instead obtain a warrant based on probable cause. (Mot. Vacate at 16.) But as demonstrated *supra*, although the Subscribers try gamely to conjure them, no “serious constitutional questions” attend the government’s straightforward § 2703(d) application in this case. And even if, as Subscribers claim, § 2703(d) gave courts the discretion to “deny applications for § 2703(d) orders” that satisfy the § 2703(d) standard (Mot. Vacate at 14), that discretion would be inapplicable here, since the Court is not being asked to rule on a pending application, but instead to vacate its already-issued order. The Subscribers have identified no provision of the SCA that gives courts the discretion to vacate valid orders in order to avoid deciding constitutional challenges. Indeed, as detailed *supra* in Section II(A), the Subscribers are seeking yet another improvised remedy not authorized by the SCA. Accordingly, the Court should decline the Subscribers’ invitation to vacate the Order.

Additionally, the alternative reading of § 2703(d) advanced by the Subscribers is contrary to the statute’s language and structure. The Subscribers’ argument relies on a Third Circuit case interpreting the “only if” language of § 2703(d) to mean that the “specific and articulable facts” requirement is a necessary condition for obtaining a 2703(d) order, but not a sufficient one. *See Third Circuit Opinion*, 620 F.3d at 319 (stating that § 2703(d) “gives the MJ the option to require a warrant showing probable cause,” although such a requirement was “an option to be used sparingly”). This alternative interpretation of § 2703(d) should be rejected because it renders

superfluous the phrase “and shall issue” in § 2703(d). The Subscribers’ “necessary but not necessarily sufficient” interpretation of § 2703(d) is equivalent to the following formulation, which omits the critical “and shall issue” language of § 2703(d): a § 2703(d) order “may be issued by any court that is a court of competent jurisdiction only if the governmental entity offers specific and articulable facts . . . .” The Subscribers’ interpretation therefore violates the cardinal principle of statutory construction that a statute ought whenever possible be construed in such a way that no “clause, sentence, or word shall be superfluous, void, or insignificant.” *Gunnells v. Healthplan Servs.*, 348 F.3d 417, 439-40 (4th Cir. 2003) (quoting *TRW Inc. v. Andrews*, 534 U.S. 19, 21 (2001) (internal quotation marks omitted)). Furthermore, the word “shall” has critical importance in a statute: “[t]he word ‘shall’ is ordinarily ‘the language of command.’” *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001). Because the Subscribers’ interpretation of § 2703(d) improperly renders “shall” superfluous, it offers no basis for the Court’s reconsideration of the Order.

Moreover, as Judge Tashima stated in his concurrence in *Third Circuit Opinion*, the Subscribers’ construction of § 2703(d) “provides no standards for the approval or disapproval of an application” for a § 2703(d) order. 620 F.3d at 319 (Tashima, J., concurring). Their interpretation would permit a magistrate judge to arbitrarily deny an application under § 2703(d) without any reasoned basis. As Judge Tashima stated, such an interpretation “is contrary to the spirit of the statute.” *Id.* The Subscribers divine a “sliding scale” at work in § 2703(d), Subscribers’ Brief at 15, but fail to delimit how far the scale may slide: indeed, under the Subscribers’ interpretation of the language of § 2703(d), a court could reject a § 2703(d) order even if the government established probable cause. In enacting the SCA, Congress could not

have intended such a chaotic and standard-less regime.

Furthermore, the Subscribers' argument that their interpretation of § 2703(d) is required by the doctrine of constitutional avoidance is mistaken. Under this doctrine, "when an Act of Congress raises a serious doubt as to its constitutionality, [courts should] first ascertain whether a construction of the statute is fairly possible by which the question may be avoided." *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (internal citations omitted). Here, as shown *supra*, the Subscribers have utterly failed to raise serious doubts about the constitutionality of § 2703(d), rendering that doctrine inapposite.

Thus, there is no reason for this Court to avoid any constitutional challenges, serious or otherwise, raised by the Subscribers. "[I]n a field like search and seizure law, where lawmakers are continually struggling to update legislation to cope with changing technology, the presumption, inherent in the doctrine of constitutional avoidance, that Congress did not intend to promulgate legislation which 'raises serious constitutional doubts,' has little applicability." *In re Application of the United States*, 632 F. Supp. 2d 202, 210 (E.D.N.Y. 2008) (internal citation omitted). For all of these reasons, the Court should reject the Subscribers' constitutional avoidance argument and decline to vacate the Order.

**E. Subscriber Jonsdottir's Status as a Member of Iceland's Parliament Does Not Insulate Twitter's Records From Disclosure Under the Order.**

Lastly, the Subscribers claim that Ms. Jonsdottir's status as a member of the Icelandic Parliament means that the Order "appears to violate Icelandic law," since she is "protected by a strong constitutional immunity in Iceland." (Mot. Vacate at 16.) The Subscribers protest that the government "is conducting a criminal investigation which sweeps in Ms. Jonsdottir's

publications in Icelandic on topics of Icelandic concern – records that could not be obtained under Icelandic law.” (Mot. Vacate at 16-17.) The Subscribers also darkly warn that this investigation “creates a perilous precedent for foreign government efforts to seek information about members of the U.S. Congress,” and urge that the Order be vacated. (Mot. Vacate at 17.)

In raising their legislative immunity claim, the Subscribers invoke the Speech or Debate Clause. (Mot. Vacate at 16 n.12). It provides, “for any Speech or Debate in either House, [Senators and Representatives] shall not be questioned in any other place.” U.S. Const. art. I, § 6, cl. 1. The Speech or Debate Clause “serves to immunize a member of Congress from being questioned about his legislative acts.” *United States v. Jefferson*, 546 F.3d 300, 304 n.2 (4<sup>th</sup> Cir. 2008). “Put simply, the Clause provides legislators with absolute immunity for their legislative activities, relieving them from defending those actions in court.” *Id.* at 310. But the constitutional protections afforded legislators are limited and circumscribed. The Speech or Debate Clause prohibits “inquiry only into those things generally said or done in the House or the Senate in the performance of official duties and into the motivation for those acts.” *United States v. Brewster*, 408 U.S. 501, 512 (1972); *United States v. Jefferson*, 534 F. Supp. 2d 645, 651 (E.D. Va. 2008) (“[T]he privilege applies only to those activities integral to a Member’s legislative function, *i.e.*, activities that are integral to the Member’s participation in the drafting, consideration, debate, and passage or defeat of legislation” (footnotes omitted)). But the Clause does not bar an “inquiry into activities that are casually or incidentally related to legislative affairs but not a part of the legislative process itself.” *Brewster*, 408 U.S. at 528. And, of course, “the Speech or Debate Clause is not a license to commit crime.” *Jefferson*, 534 F. Supp. 2d at 652.

Here, the Subscribers' assertion of legislative immunity based on Ms. Jonsdottir's status as a foreign legislator is fatally flawed, in several respects. First, of course, Ms. Jonsdottir is not a member of Congress, and thus cannot claim the protections of the Speech or Debate Clause. That Clause by its terms applies only to "Senators and Representatives." *See United States v. Gillock*, 445 U.S. 360, 366 n.5 (1980).

Second, even if apart from the Speech or Debate Clause Ms. Jonsdottir qualifies for "legislative immunity" in courts of the United States, *see E.E.O.C. v. Wash. Suburban Sanitary Comm.*, — F.3d —, 2011 WL 228591 (4<sup>th</sup> Cir. 2011) (protected legislative acts "generally bear the outward marks of public decisionmaking, including the observance of formal legislative procedures"), in this preliminary investigative proceeding there is no occasion to assert that doctrine. The Order seeks business records from Twitter, not Ms. Jonsdottir. It does not require Ms. Jonsdottir's participation or presence, or that she do anything at all. The Order does not seek sensitive or confidential information, but rather data that Ms. Jonsdottir voluntarily provided to an American corporation, and in which she has no privacy interest. The Order does not compel testimony - from any person. *Cf.* U.S. Const. art. I, § 6, cl. 1 (legislators "shall not be questioned . . ."). It does not seek content - so it is irrelevant whether Ms. Jonsdottir's Tweets were "predominantly in Icelandic," or in any other language. (Mot. Vacate at 16.) It does not seek information about any aspect of parliamentary affairs in Iceland, including any of Ms. Jonsdottir's legislative acts or activities. It does not seek information regarding other Twitter accounts known to be used by members of Iceland's parliament; the other Subscribers do not hold such status. In short, upon examination, the Subscribers' claim that Ms. Jonsdottir's status as a parliamentarian gives rise to "concerns" in this § 2703(d) proceeding is vacuous. *Cf. Wash.*

*Suburban Sanitary Comm.*, 2011 WL 228591, at \*9 (refusing to quash administrative subpoena at preliminary stage of investigation where it was unknown whether investigation would evolve into lawsuit or whether defending such a suit would require legislators' testimony or involvement).

Third, even if Ms. Jonsdottir could invoke legislative immunity here, and further could show that she used her Twitter account to communicate with her constituents about matters in Iceland's parliament, that factor is of no moment, since her Tweets to constituents were not protected legislative acts. The Founders never intended to grant legislative immunity "for defamatory statements scattered far and wide by mail, press, and the electronic media." *Hutchinson v. Proxmire*, 443 U.S. 111, 132 (1979). Moreover, a legislator's public statements, including newsletters and press releases, are "not part of the legislative function or the deliberations that make up the legislative process." *Id.* at 133. Accordingly, "transmittal of such information by press releases and newsletters is not protected by the Speech or Debate Clause." *Id.* It follows that the Subscribers cannot hope to demonstrate that Ms. Jonsdottir is entitled to legislative immunity - whatever that might mean in this § 2703(d) proceeding - based on her public Tweets.

Fourth, and finally, a legislator cannot decline to participate in a lawful criminal investigation, or prevent others from doing so, based on his or her status. In *Gravel v. United States*, 408 U.S. 606 (1972), a United States Senator moved to quash a federal grand jury subpoena served on a member of the senator's own staff. The grand jury was investigating possible crimes relating to the release and dissemination of the Pentagon Papers. It appeared that the Senator had read extensively to a subcommittee from the Pentagon Papers (which were then

classified) and had placed all 47 volumes in the public record, and had afterwards negotiated with publishers about publishing the documents. 408 U.S. at 609-10. In the grand jury investigation, the Senator intervened, citing the Speech or Debate Clause, and moved to quash the subpoena and to require the government to specify the questions to be asked his aide.

The Supreme Court held that the Senator's aide was required to testify before the grand jury. Reflecting upon the Speech or Debate Clause, the Court stated:

[The Clause], as we have emphasized, does not purport to confer a general exemption upon Members of Congress from liability or process in criminal cases. Quite the contrary is true. While the Speech or Debate Clause recognizes speech, voting, and other legislative acts as exempt from liability that might otherwise attach, it does not privilege either Senator or aide to violate an otherwise criminal law in preparing for or implementing legislative acts. If republication of these classified papers would be a crime under an Act of Congress, it would not be entitled to immunity under the Speech or Debate Clause. It also appears that the grand jury was pursuing this very subject in the normal course of a valid investigation.

408 U.S. at 626. The Court further opined that it did not "perceive any constitutional or other privilege that shields [the aide], any more than any other witness, from grand jury questions relevant to tracing the source of obviously highly classified documents that came into the Senator's possession and are the basic subject of inquiry in this case, as long as no legislative act is implicated by the questions." *Id.* at 628 (footnote omitted).

*Gravel* demonstrates that a senator cannot use his status to exempt himself from a criminal investigation, or to prevent a third party from complying with lawful investigative process. *See Brewster*, 408 U.S. at 516 (purpose of Speech or Debate Clause was not "to make Members of Congress super-citizens, immune from criminal responsibility"). Here, Ms. Jonsdottir manifestly cannot invoke her position as an Icelandic parliamentarian and thereby

block Twitter's compliance with an Order to provide non-privileged and non-content information that she voluntarily relinquished to that corporation months ago. Even if she were a member of Congress, she could not do so.

### III. Conclusion

For the reasons stated, this Court should deny the Subscribers' motion to vacate the Order of December 14, 2010.

Respectfully submitted,

Neil H. MacBride  
United States Attorney

By: /s/  
John S. Davis  
Tracy Doherty-McCormick  
Assistant United States Attorneys  
United States Attorney's Office  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
(703) 299-3700

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true copy of the foregoing Objection was filed with the Clerk of the Court on February 7, 2011, and a copy of this filing was e-mailed to opposing counsel at the following addresses:

John K. Zwierling  
Stuart Sears  
Zwierling, Liebig & Moseley, P.C.  
108 N. Alfred Street  
Alexandria, VA 22314  
[JZ@Zwierling.com](mailto:JZ@Zwierling.com)  
Counsel for Jacob Appelbaum

Johnathan Shapiro  
Greenspun, Shapiro, Davis, & Leary  
3955 Chain Bridge Rd  
Second Floor  
Fairfax, VA 22030  
[Js@greenspunlaw.com](mailto:Js@greenspunlaw.com)  
Counsel for Birgitta Jonsdottir

Nina J. Ginsberg  
Dimuro Ginsberg P.C.  
908 King Street, Suite 200  
Alexandria, VA 22314  
[nginsberg@dimuro.com](mailto:nginsberg@dimuro.com)  
Counsel for Rop Gonggrijp

Rebecca K. Glenberg  
ACLU of Virginia Foundation, Inc.  
530 E. Main Street, Suite 310  
Richmond, VA 23219  
[rglenberg@acluva.org](mailto:rglenberg@acluva.org)

/s/  
\_\_\_\_\_  
John S. Davis  
Assistant United States Attorney  
2100 Jamison Avenue  
Alexandria, VA 22314  
Phone: (703) 299-3700  
Fax: (703) 299-3982